CSD LINK ARRANGEMENT REVIEW QUESTIONNAIRE

Exercise February 2020

Date: 24 April 2020

Responding CSD: KELER Zrt.

The questionnaire aims at addressing the requirements for assessment of CSD links under the CSD Regulation (EU Regulation 909/2014 (CSDR), Regulatory Technical Standards 2017/392 (RTS) and Implementing Technical Standards 2017/394[1]).

[1] Relevant extract from the CSDR, RTS and ITS are provided in the Annex to this questionnaire.

CONTENTS

1. CREDENTIALS 3
2. RELEVANT DEVELOPMENTS (CSDR RTS 84.1 h (I)) 4
3. RISK MANAGEMENT, AUDIT, ASSET PROTECTION & CYBER RESILIENCE (CSDR 48.1, CSDR RTS 84.1) 4
4. OUTSOURCING / CRITICAL SERVICE PROVIDER (CSDR RTS 69.2) 6
5. CONFIDENTIALITY AND DATA PROTECTION (CSDR RTS 84.1 (F)) 7
6. DVP SETTLEMENT (CSDR RTS 84.1 (J)) & FINALITY (CSDR 39.4, 48.4)) 8
7. INTEGRITY OF ISSUE & RECONCILIATION (CSDR 37 & CSDR RTS 59, 64, 65, 86) 9
8. USE OF LEIs IN THE CSD SYSTEM (CSDR ITS 11.5) 10
9. SYSTEMS, COMMUNICATION ARRANGEMENTS, BUSINESS CONTINUITY AND RECOVERY PLANS (CSDR RTS 8.3, 69.1, 84.1 (G) & 84.1 (H) (II)) 10
10. SECURITIES SUBJECT TO IMMOBILISATION – ANSWER ONLY IF APPLICABLE (CSDR RTS 59.3) 12
11. ADDITIONAL NON-EU CSD QUESTIONS (CSDR RTS 84.1 (b)) 13
12. ANY ADDITIONAL COMMENT 15

ANNEX - Extract of the relevant articles 16
I. CSD Regulation (909/2014) 16
II. RTS - Delegated regulation 2017/392 19
III. CSDR ITS - Implementing Regulation 2017/394 31

1. CREDENTIALS

1.1. Respondent Information	
Name of the responding CSD **LEI of the responding CSD**	KELER Ltd 529900MPT6BHOJRPB746
LEI expiry date of the responding CSD **Address**	26th January 2021 70-72 Rákóczi str., Budapest, Hungary, H-1074
Designated responding person (Name/Title)	Ms Fruzsina Anna Gonda/ Capital Market Relations and Sales Associate
Contact details (Email/Phone)	gonda.fruzsinaanna@keler.hu / +3614836132

1.2. Participation rules / requirements (CSDR RTS[2] 84.1 a))
Please enclose your current participation rules, terms and conditions and/or requirements to other CSDs.
[File Attachment] *https://english.keler.hu/Key%20documents/Regulatory%20documents/General%20Business%20Rules/*
Have there been any changes to the rules / requirements in the past 12 months?
(X) Yes (please provide details under Comments) ( ) No
Comments:
General Business Rules (GBR) of KELER Ltd. could change for various reasons, CSDR compliance, introduction of new products, etc. The complete history of KELER GBR is available at our website.

1.3. Authorisation
What is the legislative basis for your authorisation? **Have you been authorised under the local regulation or under the EU CSDR (EU Regulation 909/2014)?** **If the local legislation is not the CSDR, has the application for its recognition as an equivalent been filed in, is planned or is already confirmed?**
( ) CSDR ( ) A law transposing provisions similar to the CSDR (e.g. in EEA countries) ( ) Legislation recognised equivalent to the CSDR by the European Commission (please provide details under Comments) (X) Other local legislation (please attach the file or include a link to the latest version of it and provide

[2] COMMISSION DELEGATED REGULATION (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.065.01.0048.01.ENG&toc=OJ:L:2017:065:TOC)

details under Comments)
Have there been any changes in your authorisation status or supervision in the past 12 months?
( ) Yes (please provide details under Comments) (X) No
Comments:
Currently the Act CXX of 2001 on the Capital Market, see attached; KELER has not applied for its recognition because once the CSDR authorisation procedure is completed, CSDR will be applicable. At the end of September 2017, KELER submitted its authorization request under the CSDR to the supervisory authority (Central Bank of Hungary). The authorisation procedure is in progress.

2. RELEVANT DEVELOPMENTS (CSDR RTS 84.1 h (i))

2.1. Were there any market, IT developments or any significant development in your local legislation (not covered under question 1.3) over the last 12 months that could affect your systems / operations?
Market developments: (X) Yes (please describe under Comments) ( ) No IT developments: (X) Yes (please describe under Comments) ( ) No Local legislation developments: ( ) Yes (please describe under Comments) (X) No
Comments:
-Implementation of Real-Time Payment System, made it possible to transfer money with maximum value of 10 million HUF within 5 seconds on a 365/7/24 basis. –Within the scope of the KELER Service Development Program KELER plans to implement a new IT architecture. The most important feature of the new architecture is that the services required for the business operations are provided by functionally well-defined, autonomous, but strictly cooperative modules. The program is aiming at the gradual replacement of the functionalities covered by the current systems. One of the main objectives of the project are to achieve full T2S harmonization, CSDR compliance, SDR compliance, developments related to fee calculation and the development of KELER internal reports. - With the Shareholders Rights Directive compliance project, of KELER is the Shareholders Rights Directive complianceKELER heads the initiative of harmonizing Hungarian Corporate Action standards with the international standard market practices. - -KELER will provide solution for trade reporting under SFTR from July 2020. -KELER is in the process of acquiring accreditation for LEI code issuance. In order to reach this goal, KELER is developing its IT system to integrate the activity.

3. RISK MANAGEMENT, AUDIT, ASSET PROTECTION & CYBER RESILIENCE (CSDR 48.1, CSDR RTS 84.1)

3.1. Risk Management
Do you have an Enterprise Risk Management framework implemented in your CSD?
(X) Yes ( ) No
Please briefly describe the your CSD's approach to risk management.
Comments:
Article 47 of the CSDR requires that the central securities depository must cover enterprise (business) risks with capital. Risks are assessed and identified within the context of a strategy, by preparing business plans based on multiple potential scenarios. Controlling department is responsible for monitoring and reporting business risks. This means the regular back-testing of business plans in the strategy and reporting the results to the Management. In addition, the Management also receives regular information about changes in costs and revenues. KELER's Management is responsible for managing enterprise risks.

3.2. Asset protection
How does your CSD ensure protection of assets held across the link? (question relevant for both, EEA and EU third-country CSDs, CSDR 84.1 e))
Please enclose the legal assessment (i) of the entitlement on securities held across the link, including the law applicable to proprietary aspects, the nature of rights and the possibility of encumbering the assets, as well as (ii) of the impact of insolvency proceedings opened against your CSD on our CSD regarding the segregation requirements, settlement finality, procedures and time-limits to claim securities in your jurisdiction.
In the case of liquidation procedure (or bankruptcy) initiated against KELER, the securities and cash of its participants shall not be included in the liquidation assets thereof. The general rules relating to insolvency law to be applied are set out in Act XLIX of 1991 on Bankruptcy Proceedings and Liquidation Proceedings, while special provisions different from these are set out in Section 345 of Act CXX of 2001 on the Capital Market. The protection related to the segregation of securities accounts can be inferred from these rules. During the liquidation of KELER, securities registered in securities accounts of Account Holders and their clients maintained by KELER are excluded from assets to be liquidated. During potential liquidation proceedings, the monetary claim which replaces the securities claim of the Account Holder and its client is to be managed identically to the original securities claim. During potential liquidation proceedings, the security deposit specified in Section 338 of the Act CXX of 2001 on the Capital Market is excluded from the assets of KELER to be liquidated. If the assets which constitute property of Account Holders and their clients cannot be returned to them, or can only be returned in part, then – deviating from the priorities set out in Section 57 of the Act XLIX of 1991 on Bankruptcy Proceedings and Liquidation Proceedings – after settling liquidation costs first, these claims must be settled from the assets of KELER. If secondary securities were issued, then during liquidation proceedings the primary security shall be handled as a security deposited by the owners of the secondary security, which belongs to the participants and is also excluded from the assets to be liquidated. The Supervising Authority shall order a complete ban on payouts from the submission date of the application for liquidation, if the assets to be liquidated are lawful and the Supervising Authority deems that suitable management of the interests of creditors, Account Holders and their clients is not

ensured.

Segregation, therefore, has practically no effect in terms of insolvency law, thus protection remains the same when securities accounts are segregated.

See the quoted regulation attached.

Comments:

-

3.3. Insolvency (CSDR RTS 26 b, 36 d)
Please briefly explain the framework that would govern (the very improbable) insolvency of your CSD.
According to the Act CXX of 2001 on Capital Market the collateral and deposit determined in the Act are not part of the liquidation asset of the institution. The securities deposited by the participants at the central depository and the securities registered in the participants' securities accounts or securities deposit accounts are also not part of the liquidation asset of the institution. For further information see point 3.2.
Comments:
-

3.4. Cyber resilience (CSDR RTS 70.9, 75.5, 78.1)
Are cyber resilience measures undertaken by your CSD?
(X) Yes ( ) No
Please briefly describe the your CSD's approach to cyber resilience. What is the level of maturity of these measures?
KELER has established a comprehensive cyber resilience framework. Based on formally accepted cyber resilience strategic and regular risk assessments, the necessary technical, operational and human resource related measurements has been implemented to ensure the protection and continuity of KELER operation day-by-day. Based on independent audit results, a mature level has been achieved.
Comments:

4. OUTSOURCING / CRITICAL SERVICE PROVIDER (CSDR RTS 69.2)

4.1. Are there any functions or duties on which you rely on critical service providers? If yes, please provide details of such critical service providers and the functions/duties on which you rely on them.
(X) Yes ( ) No
Comments:
The handling of Polish Corporate Actions is outsourced to Societe Generale SS Poland – KELER also has a signed and valid Service Level Agreement with SGSS. KELER outsourced some of its IT development activities – according to its outsourcing rules, backed up by contracts.

4.2.	**Do you outsource any aspect of the settlement or related services or operations to third parties? If yes, please provide details.**
( ) Yes (X) No	
Comments:	
Not applicable.	

5. CONFIDENTIALITY AND DATA PROTECTION (CSDR RTS 84.1 (F))

5.1.	**Please enclose the documentation/arrangements, which provide for the confidentiality of the information with regard to your operations.**
Information Security Policy, Confidentiality Regulation and Data Protection Regulation of KELER Group. These Regulations are confidential - not publicly available.	
Comments:	
KELER processes and controls all kinds of data that become known to it in line with the provisions of the applicable regulations, the GDPR, the Act CXII of 2011 on Informational Self-determination on Freedom of Information, and the Regulatory Documents. The detailed Privacy Policy is available on the website of KELER in the Data Protection menu item.	

5.2.	**Do your employees sign a confidentiality clause?**
(X) Yes ( ) No	
Comments:	
-	

5.3.	**Do you have a formal data protection policy? If yes, please attach a copy or alternatively provide a description of such policies.**
(X) Yes ( ) No (please comment under Comments)	
Please upload files here:	
https://english.keler.hu/Privacy%20Policy/	
Comments:	
The detailed Privacy Policy is available on the website of KELER in the Data Protection menu item.	

5.4.	**Does your jurisdiction have formal data protection or privacy laws/regulations?**
(X) Yes, it is EU GDPR ( ) Yes, although it is different/supplementing an EU GDPR (please provide the details of the laws under Comments) ( ) No (please comment under Comments)	
Comments:	
https://english.keler.hu/Privacy%20Policy/	

5.5.	**Are you required to report data breaches to your regulators?**
(X) Yes ( ) No	
Comments:	
-	

5.6.	**In the last 12 months have you reported any data breaches to your regulators? If yes, please provide details.**
( ) Yes (please provide details under Comments) (X) No	
Comments:	
-	

6. DVP SETTLEMENT (CSDR RTS 84.1 (J)) & FINALITY (CSDR 39.4, 48.4))

6.1.	**Is DVP settlement in your systems conducted via accounts at the central bank of the relevant settlement currency?**
(X) Yes ( ) No (please provide details under Comments)	
Comments:	
Local custodian banks use their central bank HUF main account for DVP settlement, on which KELER has entitlement to deduct and credit. Broker-dealers though have the possibility to keep their HUF accounts at the Central Bank, still keep their cash accounts in the books of KELER, and hence the settlement takes place in our books in that case.	

6.2.	**Please disclose the rules governing the moment of entry and irrevocability of transfer orders and finality of cash and securities transfers related to settlement in your system.**
Moment of entry:	
KELER considers the order for the value date concerned received order (either submitted on the same day or with value dating or recycled from earlier) on the day if the order - is successfully received within the cut-off times, - is submitted in the manner and with the content determined in the SLA (i.e. the order is not rejected for reasons of logic, format or content), and - the related verification of cover was successful.	
Moment of irrevocability:	
When the initial instruction is matched, the settlement process started, and there is no way to cancel it: meaning the settlement actually took place in KELER's systems. In accordance to the Finality Directive, book-entry transfers within KELER's books are final and irrevocable.	
Moment of finality:	
When the settlement actually takes place in KELER's systems. In accordance to the Finality Directive, book-entry transfers within KELER's books are final and irrevocable.	

6.3.	**Please confirm that retransfer of securities before a transfer is final is prohibited in your systems? (CSDR 48.4)**

(X) Yes ( ) No (please provide details under Comments)
Comments:
-

7. INTEGRITY OF ISSUE & RECONCILIATION (CSDR 37 & CSDR RTS 59, 64, 65, 86)

7.1.	**Please confirm that you conduct daily reconciliation to verify the number of securities making up a securities issue or part of a securities issue in your systems is equal to the sum of securities recorded on the securities accounts of your participants; and the results of such reconciliation are available to your participants (and linked CSDs) after the closure of the settlement day and in any case prior to the start of the next settlement day you endeavour to resolve any mismatches and inconsistencies revealed by the reconciliation process before the beginning of settlement on the following business day.**
(X) Yes ( ) No (please provide details of the relevant processes under Comments)	
Comments:	
-	

7.2.	**If the reconciliation process reveals undue creation or deletion of securities that is not solved by the end of the following business day and you decide to suspend from settlement the securities issue, please describe the process and means used to inform your participants and other CSDs holding securities with you.**
Although KELER does not expect that any event raising the suspicion of deviation would occur, KELER analyses all cases of non-compliance and controversy that may result from reconciliation and intends to solve them on the day of occurrence. If it can be concluded based on the reconciliation that the creation or cancellation of securities was unjustified, and KELER does not sort out the issue until the end of the following settlement day, KELER suspends the settlement of the securities series concerned until the unjustified securities creation or cancellation is remedied, and it requests the trading venue concerned to suspend it also. KELER informs its participants and the authorities involved without delay via phone and/or email [beyond the regular communication channel (KID / SWIFT)]. After the correction of any deviation, the suspension of the securities series is terminated, thus ensuring continuous trading of the securities concerned.	

7.3.	**Please describe the process and means used to inform your participants and other CSDs holding securities with you after undue creation or deletion of securities has been remedied and settlement is resumed.**
KELER informs its participants and other CSDs involved through the agreed communication channels (KID / SWIFT) and via phone and/or email in due course. However please note that KELER-s system and instruction handing is set up in a way, that there is no chance for a securities account to receive undue	

securities.

7.4.	**Do you currently transmit to your participants (including other CSDs holding securities with you) information on the processing of corporate actions? If not, please describe under Comments the enhancements planned in this regard, as relevant.**
(X) Yes ( ) No	
Comments:	
KELER sends notifications of upcoming CA events electronically in accordance with the contract/ Service Level Agreement concluded with the Participant.	

8. USE OF LEIs IN THE CSD SYSTEM (CSDR ITS 11.5)

8.1.	**Do you identify CSDs, CSD participants, settlement banks and issuers (as per point CSDR ITS 11.5(d)) with LEIs in your system?**
(X) Yes ( ) No	
Comments:	
-	

8.2.	**In case the response to the first question in the section is "Yes", please describe your review processes to ensure issuers' LEIs are renewed annually?**
In line with the expectations of ESMA, after the CSDR license is received, KELER will validate that the LEIs provided by issuer participants are the identifiers of the appropriate legal entities and the identifiers are valid. KELER will send alert to issuer participants before the expiry date of LEI Codes and ask them to make the necessary steps for the renewal.	

8.3.	**In case the response to the first question in the section is "Yes", please describe the actions you would take should an issuer fail to renew its LEI annually?**
Issuers with invalid LEI codes will cease to be eligible to use KELER's services till the renewal process has been taken place.	

9. SYSTEMS, COMMUNICATION ARRANGEMENTS, BUSINESS CONTINUITY AND RECOVERY PLANS (CSDR RTS 8.3, 69.1, 84.1 (G) & 84.1 (H) (II))

9.1.	**Please describe the communication standards and procedures applicable to your settlement and other core systems.**
KELER provides electronic communication through: • its KID system (using ISO standard format messages) • the SWIFT system (in line with the KELER SWIFT Rule Book) or the interface available on the website of KELER (eKID)	

9.2.	**Where SWIFT communication is not possible which alternative means of communication could be used between you and your participants (including other CSDs)?**
(X) Fax (Encrypted fax number: +36 1 352 1042) (X) E-mail (Email address: accountmanagement@keler.hu; Correspondence is through forced TLS	

connection, and files/mails can be sent in SMIME encrypted mail, or in AES 256 encrypted zip files. In the latter case it is recommended that sensitive data is stored in the encrypted zip only, additionally, the password should be of at least 12 characters, include special characters, and should be changed monthly. If any electronic communication client relationship system is not available, the participant acknowledges that in case of substituting email advice KELER is not liable for damage arising from sending unencrypted advice or forwarding the advice without digital authentication.) ( ) Other (please describe)

9.3.	**Do you have a business continuity plan which can you can share with us?**
(X) Yes ( ) No (please provide details under comments)	
Please upload files here: *https://english.keler.hu/Key%20documents/Regulatory%20documents/Management%20of%20Extraordinary%20Situations%20of%20KELER%20Group/*	
Comments:	
-	

9.4.	**Recovery plan (CSDR 22.2, CSDR RTS 8.3)**
Does your CSD have a recovery plan?	
(X) Yes ( ) No (please provide details under comments)	
Please upload files here or briefly describe measures your CSD could take that may have an impact on the linked CSD(s)	
KELER's recovery plan prepares KELER for possible financial difficulties, system deteriorations and any pre plannable situation that can cause system and KELER downtime. The plan includes restoration scenarios in a timely manner. The plan is aligned with KELER's risk management framework. Through the recovery plan, KELER has set up a governance framework that detects a stress situation and ensures its operation in a crisis.	
Comments:	
-	

9.5.	**Please describe the media used to communicate with your participants (including other CSDs holding securities with you) on:**
a)	**operational issues**
b)	**activation of business continuity plan**
c)	**operational issues being remedied, or plan being deactivated.**
a) SWIFT, KID, email, telephone and publication on our website b) KID, email, telephone and publication on our website c) KID, email, telephone and publication on our website	

9.6.	**Please provide the contact details of the person who can be contacted in case of business contingency both within business hours and outside business hours.**
KELER Group contact details are:	

KELER Group switchboard: (+36-1) 483-6100 KELER Group Service Desk phone number: (+36-1) 483-6120 KELER Group telefax number: (+36-1) 342–3539 KELER Group Service Desk e-mail: servicedesk@keler.hu KELER Group central e-mail: keler@keler.hu KELER Group contact list by departments

10. SECURITIES SUBJECT TO IMMOBILISATION – ANSWER ONLY IF APPLICABLE (CSDR RTS 59.3)

10.1. Please confirm that your vault security features include the following:	
Security Guards	(X) Yes ( ) No
24-hour closed-circuit camera surveillance	(X) Yes ( ) No
Dual control over all activities	(X) Yes ( ) No
Monitoring of access via a log book	(X) Yes ( ) No
Alarms	(X) Yes ( ) No
Panic buttons	(X) Yes ( ) No
Movement detectors	(X) Yes ( ) No
Timed locks	(X) Yes ( ) No
Fire suppression systems	(X) Yes ( ) No
Flood control systems	(X) Yes ( ) No
Earthquake-resistant structures	(X) Yes ( ) No
Other (please list additional features)	Wall-drilling and wall-demolition sensors

10.2. Please state the location of the vault.
The location of the vault is in the centre of Budapest (VIth district).

10.3. Do you have procedures and controls for physical transportation of securities?
(X) Yes ( ) No
Comments:
-

10.4. Were there any exceptions for the vault safeguards noted in your last audit? If yes, please outline the exceptions and steps taken to rectify.
( ) Yes

(X) No
Comments:
-

10.5.	**In the last 12 months, have you experienced any breaches in these safeguards? If yes, please describe how they were addressed / resolved?**
( ) Yes (X) No	
Comments:	
-	

10.6.	**Do you outsource the safekeeping of physical assets? If "Yes" please provide further details under Comments.**
(X) Yes ( ) No	
Comments:	
The vault services are outsourced to an external bank, Erste Bank.	

10.7.	**Please outline how you monitor vault capacity levels and advise what capacity the vault is operating to.**
The current capacity utilisation rate is 50%. On request the vault capacity can be increased. KELER Ltd. does annual inventory check for reconciliation and also on every delivery in, there is a capacity check done.	

10.8.	**Please outline your Business Continuity Plan should the operation of your vault become impaired.**
We follow the provisions of our Business Continuity Plan (please refer to the point 8.3.).	

10.9.	**How frequently are physical securities counted and reconciled with your records?**
( ) Quarterly ( ) Semi annually (X) Annually ( ) Other (please specify)	
Comments:	
-	

11. ADDITIONAL NON-EU CSD QUESTIONS (CSDR RTS 84.1 (B))

11.1.	**Financial soundness and audit (CSDR RTS 84.1 (b)- financial soundness)**
Please enclose the latest internal, external and regulatory audits.	
N/A, KELER is an EU CSD.	
How frequently is your CSD's activities audited by your internal and external auditors, relevant authorities? Please provide the date of the last internal, external and regulatory audits.	
Comments:	

N/A, KELER is an EU CSD. Please enclose your latest annual report in English including your latest financial figures
N/A, KELER is an EU CSD.

11.2. Governance (CSDR RTS 84.1 (b)) **Please outline your governance arrangements** **The CSD with which an EU CSD has a link, should have the governance arrangements outlining the following:** **(a) the composition, role, responsibilities, procedures for appointment, performance assessment and accountability of the Board and of its committees;** **(b) the structure, role, responsibilities, procedures for appointment, performance assessment and accountability of the Management Committee;** **(c) the reporting lines between the Board & the Management Committee.**	
Please briefly explain the governance arrangements in place in your CSD in that respect.	
N/A, KELER is an EU CSD.	
Comments:	
N/A, KELER is an EU CSD.	
Does your organisation have an internal Code of Conduct?	( ) Yes ( ) No
Do you have a fraud prevention & insider dealing Policy in place?	( ) Yes ( ) No
Do you have a Conflict of Interest Policy & Register in place?	( ) Yes ( ) No

11.3. Processing capacity (CSDR RTS 84.1 (b)) **How often do you assess and test your capacity utilisation under stress conditions?**	
Comments:	
( ) Annually ( ) Every two years ( ) Every three years ( ) Every four years or more ( ) Never	
Please state your daily degree of capacity (percentage on average and at peak) utilisation with regard to:	
Settlement	% on average: % at peak:
Asset servicing (corporate actions, income)	% on average: % at peak:

11.4. Operational reliability (CSDR RTS 84.1 (b)) **In the last 12 months have you had system outages or slowdowns that have impacted your ability to service your participants? If yes, please detail how many such events there have been.**
( ) Yes ( ) No

Comments: **What has been your average settlement system uptime over the last 12 months?**
N/A, KELER is an EU CSD.
Have you suffered any claims due to operational loss over the past 3 years? If so, please describe the case.
N/A, KELER is an EU CSD.

12. ANY ADDITIONAL COMMENT

12.1. Please include any additional information and comment that are important in the context of the CSDR due diligence that could not fit under the questions above
Disclaimer: Please note that KELER does not take any responsibility for the accuracy, content, completeness, legality, reliability of the information or for any kind of information error or omission in this Due Diligence Questionnaire. No liability (whether direct, indirect, or consequential, in contract, tort or otherwise) will be assumed by KELER for any costs, expenses, losses or liabilities incurred in connection with the use of (or the inability to use) this Due Diligence Questionnaire.

ANNEX - EXTRACT OF THE RELEVANT ARTICLES

I. CSD REGULATION (909/2014)[3]

Article 37

Integrity of the issue

1. A CSD shall take appropriate reconciliation measures to verify that the number of securities making up a securities issue or part of a securities issue submitted to the CSD is equal to the sum of securities recorded on the securities accounts of the participants of the securities settlement system operated by the CSD and, where relevant, on owner accounts maintained by the CSD. Such reconciliation measures shall be conducted at least daily.

2. Where appropriate and if other entities are involved in the reconciliation process for a certain securities issue, such as the issuer, registrars, issuance agents, transfer agents, common depositories, other CSDs or other entities, the CSD and any such entities shall organise adequate cooperation and information exchange measures with each other so that the integrity of the issue is maintained.

3. Securities overdrafts, debit balances or securities creation shall not be allowed in a securities settlement system operated by a CSD.

4. ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the reconciliation measures a CSD is to take under paragraphs 1, 2 and 3.

ESMA shall submit those draft regulatory technical standards to the Commission by 18 June 2015.

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.

Article 38

Protection of securities of participants and those of their clients

1. For each securities settlement system it operates, a CSD shall keep records and accounts that shall enable it, at any time and without delay, to segregate in the accounts with the CSD, the securities of a participant from those of any other participant and, if applicable, from the CSD's own assets.

2. A CSD shall keep records and accounts that enable any participant to segregate the securities of the participant from those of the participant's clients.

3. A CSD shall keep records and accounts that enable any participant to hold in one securities account the securities that belong to different clients of that participant ('omnibus client segregation')

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0909

4. A CSD shall keep records and accounts that enable a participant to segregate the securities of any of the participant's clients, if and as required by the participant ('individual client segregation').

5. A participant shall offer its clients at least the choice between omnibus client segregation and individual client segregation and inform them of the costs and risks associated with each option.

However, a CSD and its participants shall provide individual clients segregation for citizens and residents of, and legal persons established in, a Member State where required under the national law of the Member State under which the securities are constituted as it stands at 17 September 2014. That obligation shall apply as long as the national law is not amended or repealed and its objectives are still valid.

6. CSDs and their participants shall publicly disclose the levels of protection and the costs associated with the different levels of segregation that they provide and shall offer those services on reasonable commercial terms. Details of the different levels of segregation shall include a description of the main legal implications of the respective levels of segregation offered, including information on the insolvency law applicable in the relevant jurisdictions.

7. A CSD shall not use for any purpose securities that do not belong to it. A CSD may however use securities of a participant where it has obtained that participant's prior express consent. The CSD shall require its participants to obtain any necessary prior consent from their clients.

Article 39

Settlement finality

1. A CSD shall ensure that the securities settlement system it operates offers adequate protection to participants. Member States shall designate and notify the securities settlement systems operated by CSDs according to the procedures referred to in point (a) of Article 2 of Directive 98/26/EC.

2. A CSD shall ensure that each securities settlement system that it operates defines the moments of entry and of irrevocability of transfer orders in that securities settlement system in accordance with Articles 3 and 5 of Directive 98/26/EC.

3. A CSD shall disclose the rules governing the finality of transfers of securities and cash in a securities settlement system.

4. Paragraphs 2 and 3 shall apply without prejudice to the provisions applicable to CSD links, and without prejudice to paragraph 8 of Article 48.

5. A CSD shall take all reasonable steps to ensure that, in accordance with the rules referred to in paragraph 3, finality of transfers of securities and cash referred to in paragraph 3 is achieved either in real time or intra-day and in any case no later than by the end of the business day of the actual settlement date.

6. Where the CSD offers the services referred to in Article 40(2), it shall ensure that the cash proceeds of securities settlements shall be available for recipients to use no later than by the end of the business day of the intended settlement date.

7. All securities transactions against cash between direct participants in a securities settlement system operated by a CSD and settled in that securities settlement system shall be settled on a DVP basis.

Article 48

CSD links

1. Before establishing a CSD link and on an ongoing basis once the CSD link is established, all CSDs concerned shall identify, assess, monitor and manage all potential sources of risk for themselves and for their participants arising from the CSD link and take appropriate measures to mitigate them.

2. CSDs that intend to establish links shall submit an application for authorisation to the competent authority of the requesting CSD as required under point (e) of Article 19(1) or notify the competent and relevant authorities of the requesting CSD as required under Article 19(5).

3. A link shall provide adequate protection to the linked CSDs and their participants, in particular as regards possible credits taken by CSDs and the concentration and liquidity risks as a result of the link arrangement.

A link shall be supported by an appropriate contractual arrangement that sets out the respective rights and obligations of the linked CSDs and, where necessary, of the CSDs' participants. A contractual arrangement with cross-jurisdictional implications shall provide for an unambiguous choice of law that govern each aspect of the link's operations.

4. In the event of a provisional transfer of securities between linked CSDs, retransfer of securities prior to the first transfer becoming final shall be prohibited.

5. A CSD that uses an indirect link or an intermediary to operate a CSD link with another CSD shall measure, monitor, and manage the additional risks arising from the use of that indirect link or intermediary and take appropriate measures to mitigate them.

6. Linked CSDs shall have robust reconciliation procedures to ensure that their respective records are accurate.

7. Links between CSDs shall permit DVP settlement of transactions between participants in linked CSDs, where practical and feasible. Detailed reasons for any CSD link not allowing for DVP settlement shall be notified to the relevant and competent authorities.

8. Interoperable securities settlement systems and CSDs, which use a common settlement infrastructure shall establish identical moments of:

(a) entry of transfer orders into the system;

(b) irrevocability of transfer orders.

The securities settlement systems and CSDs referred to in the first subparagraph shall use equivalent rules concerning the moment of finality of transfers of securities and cash.

9. By 18 September 2019 all interoperable links between CSDs operating in Member States shall be, where applicable, DVP-settlement supporting links.

10. ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the conditions provided for in paragraph 3 under which each type of link arrangement provides for adequate protection of the linked CSDs and of their participants, in particular where a CSD intends to participate in the securities settlement system operated by another CSD, the monitoring and managing of additional risks referred to in paragraph 5 arising from the use of intermediaries, the reconciliation methods referred to in paragraph 6, the cases where DVP settlement through CSD links is practical and feasible as provided for in paragraph 7 and the methods of assessment thereof.

ESMA shall submit those draft regulatory technical standards to the Commission by 18 June 2015.

Powers is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.

II. RTS - DELEGATED REGULATION 2017/392[4]

Article 8

Financial reports, business plan, and recovery plan

1. An application for authorisation shall include the following financial and business information to enable the competent authority to assess compliance of the applicant CSD with Articles 44, 46 and 47 of Regulation (EU) No 909/2014:

(a)financial reports including a complete set of financial statements for the preceding three years, and the statutory audit report on the annual and consolidated financial statements within the meaning of Directive 2006/43/EC of the European Parliament and of the Council ([6]), for the preceding three years;

(b)where the applicant CSD is audited by an external auditor, the name and the national registration number of the external auditor;

(c)a business plan, including a financial plan and an estimated budget that foresees various business scenarios for the services provided by the applicant CSD, over a reference period of at least three years;

(d) any plan for the establishment of subsidiaries and branches and their location;

(e)a description of the business activities that the applicant CSD plans to carry out, including the business activities of any subsidiaries or branches of the applicant CSD.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.065.01.0048.01.ENG&toc=OJ:L:2017:065:TOC)

2. Where historical financial information referred to in point (a) of paragraph 1 is not available, an application for authorisation shall include the following information about the applicant CSD:

(a) evidence that demonstrates sufficient financial resources during six months after the granting of an authorisation;

(b) an interim financial report;

(c) statements concerning the financial situation of the applicant CSD, including a balance sheet, income statement, changes in equity and in cash flows and a summary of accounting policies and other relevant explanatory notes;

(d) audited annual financial statements of any parent undertaking for the three financial years preceding the date of the application.

3. **The application shall include a description of an adequate recovery plan to ensure continuity of the applicant CSD's critical operations referred to in Article 22(2) of Regulation (EU) No 909/2014 including:**

(a) a summary that provides an overview of the plan and its implementation;

(b) the identification of the critical operations of the applicant CSD, stress scenarios and events triggering recovery, and a description of recovery tools to be used by the applicant CSD;

(c) an assessment of any impact of the recovery plan on stakeholders that are likely to be affected by its implementation;

(d) an assessment of the legal enforceability of the recovery plan that takes account of any legal constraints imposed by Union, national or third country legislation.

Article 25

Integrity of the issue

An application for authorisation shall include information concerning the applicant CSD's rules and procedures for ensuring the integrity of securities issues referred to in Article 37 of Regulation (EU) No 909/2014 and Chapter IX of this Regulation.

Article 26

Protection of participants' and their clients' securities

An application for authorisation shall include the following information concerning the measures put in place to protect the securities of the applicant CSD's participants and those of their clients in accordance with Article 38 of Regulation (EU) No 909/2014:

(a) the rules and procedures to reduce and manage the risks associated with the safekeeping of securities;

(b) a detailed description of the different levels of segregation offered by the applicant CSD, a description of the costs associated with each level, the commercial terms on which they are

offered, their main legal implications and the applicable insolvency law;

(c)the rules and procedures for obtaining the consents referred to in Article 38(7) of Regulation (EU) No 909/2014.

Article 27

Settlement finality

An application for authorisation shall contain information concerning the rules on settlement finality put in place by the applicant CSD in accordance with Article 39 of Regulation (EU) No 909/2014.

Article 36

CSD links

Where the applicant CSD has established or intends to establish CSD links, the application for authorisation shall contain the following information:

(a)a **description of the CSD links** accompanied by assessments of potential sources of risks arising from those link arrangements by the applicant CSD;

(b)the **expected or actual settlement volumes and values** of the settlement performed within the CSD links;

(c)the **procedures concerning the identification, assessment, monitoring and management of all potential sources of risk** for the applicant CSD and for its participants arising from the link arrangement and the appropriate measures put in place to mitigate them;

(d)an assessment of the applicability **of insolvency laws applicable** to the operation of a CSD link and their implications for the applicant CSD;

(e)other relevant information requested by the competent authority for assessing the compliance of CSD links with the requirements provided in Article 48 of Regulation (EU) No 909/2014 and Chapter XII of this Regulation.

Article 59

General reconciliation measures

1. A CSD shall perform the reconciliation measures referred to in Article 37(1) of Regulation (EU) No 909/2014 for each securities issue recorded in securities accounts centrally and not centrally maintained by the CSD.

The CSD shall compare the previous end-of-day balance with all the settlements processed during the day and the current end-of-day balance for each securities issue and securities account centrally or not centrally maintained by the CSD.

A CSD shall use double-entry accounting, according to which for each credit entry made on a securities account maintained by the CSD, centrally or not centrally, there is a corresponding debit entry on another securities account maintained by the same CSD.

2. The audits referred to in Article 26(6) of Regulation (EU) No 909/2014 shall ensure that the records of a CSD related to securities issues are accurate, and that its reconciliation measures referred to in Article 37(1) of Regulation (EU) No 909/2014 and the measures concerning cooperation and exchanges of information with third parties related to reconciliation referred to in Article 37(2) of Regulation (EU) No 909/2014 are adequate.

3. **Where the reconciliation process concerns securities subject to immobilisation, a CSD shall put in place adequate measures to protect the physical securities from theft, fraud, and destruction. Those measures shall at least include the use of vaults whose design and location ensure a high level of protection against floods, earthquakes, fire and other disasters.**

4. Audits referred to in Article 26(6) of Regulation (EU) No 909/2014 with respect to the vaults, including physical inspections, shall be performed at least annually. The CSD shall share the results of those audit controls with the competent authority.

Article 60

Reconciliation measures for corporate actions

1. A CSD shall not determine the entitlements to the proceeds of a corporate action on stock that would change the balance of securities accounts maintained by the CSD until the reconciliation measures specified in Article 59 and in Articles 61, 62 and 63 are completed.

2. When a corporate action has been processed, a CSD shall ensure that all securities accounts maintained by the CSD, centrally or not centrally, are updated.

Article 64

Additional measures where other entities are involved in the reconciliation process

1. A CSD shall review at least annually its cooperation and information exchange measures with other entities referred to in Articles 61, 62 and 63. This review may be conducted in parallel with a review of the CSD link arrangements. When required by the competent authority, the CSD shall implement other cooperation and information exchange measures in addition to those specified in this Regulation.

2. When a CSD establishes links, they shall comply with the additional requirements provided in Article 86.

3. A CSD shall require its participants to reconcile their records with the information received from that CSD on a daily basis.

4. For the purposes of paragraph 3, the CSD shall provide participants on a daily basis the following information specified for each securities account and for each securities issue:

(a)the aggregated balance of a securities account at the beginning of the respective business day;

(b)the individual transfers of securities in or from a securities account during the respective

business day;

(c) the aggregated balance of a securities account at the end of the respective business day.

The CSD shall provide the information referred to in the first subparagraph at the request of other holders of securities accounts maintained by the CSD, centrally or not centrally, where that information is necessary for the reconciliation of those holders' records with the records of the CSD.

5. A CSD shall ensure that, upon its request, its participants, other holders of accounts in the CSD and the account operators provide the CSD with the information that the CSD deems necessary to ensure the integrity of the issue, in particular to solve any reconciliation problems.

For the purposes of this paragraph, 'account operator' shall mean an entity that is contracted by a CSD to record book entries into its securities accounts.

Article 65

Problems related to reconciliation

1. A CSD shall analyse any mismatches and inconsistencies resulting from the reconciliation process and endeavour to solve them before the beginning of settlement on the following business day.

2. Where the reconciliation process reveals an undue creation or deletion of securities, and the CSD fails to solve this problem by the end of the following business day, the CSD shall suspend the securities issue for settlement until the undue creation or deletion of securities has been remedied.

3. In the event of suspension of the settlement, the CSD shall inform without undue delay its participants, competent authority, relevant authorities and all other entities involved in the reconciliation process referred to in Articles 61, 62 and 63.

4. The CSD shall take without undue delay all the necessary measures to remedy the undue creation or deletion of securities and shall inform its competent authority and relevant authorities with regard to the measures taken.

5. The CSD shall inform without undue delay its participants, competent authority, relevant authorities and the other entities involved in the reconciliation process that are referred to in Articles 61, 62 and 63, when the undue creation or deletion of securities has been remedied.

6. Where a securities issue is suspended from settlement, the settlement discipline measures set out in Article 7 of Regulation (EU) No 909/2014 shall not apply in relation to that securities issue for the period of suspension.

7. The CSD shall resume settlement as soon as the undue creation or deletion of securities has been remedied.

8. Where the number of instances of undue creation or deletion of securities referred to in paragraph 2 is higher than five per month, the CSD shall send within one month the competent authority and the relevant authorities a proposed plan of measures for mitigating the occurrence of similar instances. The CSD shall update the plan and shall provide a report on its

implementation to the competent authority and the relevant authorities on a monthly basis, until the number of instances referred to in paragraph 2 falls below five per month.

Article 69

Operational risks that may be posed by other CSDs or market infrastructures

1. **A CSD shall ensure that its systems and communication arrangements with other CSDs or market infrastructures are reliable, secure and designed to minimise operational risks.**

2. Any arrangement that a CSD enters into with another CSD or another market infrastructures shall provide that:

(a) the other CSD or other financial market infrastructure discloses to the CSD any critical service provider on which the other CSD or market infrastructure relies;

(b) the governance arrangements and management processes in the other CSD or other market infrastructure do not affect the smooth provision of services by the CSD, including the risk-management arrangements and the non-discriminatory access conditions.

Article 70

Operational risk-management system and framework

1. As part of the policies, procedures and systems referred to in Article 47, a CSD shall have in place a well-documented framework for the management of operational risk with clearly assigned roles and responsibilities. A CSD shall have appropriate IT systems, policies, procedures and controls to identify, measure, monitor, report on and mitigate its operational risk.

2. The management body and the senior management of a CSD shall determine, implement and monitor the risk-management framework for operational risks referred to in paragraph 1, identify all of the CSD's exposures to operational risk and track relevant operational risk data, including any cases where material data is lost.

3. A CSD shall define and document clear operational reliability objectives, including operational performance objectives and committed service-level targets for its services and securities settlement systems. It shall have policies and procedures in place to achieve those objectives.

4. A CSD shall ensure that its operational performance objectives and service-level targets referred to in paragraph 3 include both qualitative and quantitative measures of operational performance.

5. A CSD shall regularly monitor and assess whether its established objectives and service-level targets are met.

6. A CSD shall have rules and procedures in place that ensure that the performance of its securities system is reported regularly to senior management, members of the management body, relevant committees of the management body, user committees and the competent authority.

7. A CSD shall periodically review its operational objectives to incorporate new technological and business developments.

8. A CSD's operational risk-management framework shall include change-management and project-management processes to mitigate operational risk arising from modifications to operations, policies, procedures and controls put in place by the CSD.

9. A CSD's operational risk-management framework shall include a comprehensive framework for physical security and information security to manage the risks that the CSD faces from attacks**, including cyber-attacks**, intrusions and natural disasters. That comprehensive framework shall enable the CSD to protect the information at its disposal from unauthorised access or disclosure, ensure data accuracy and integrity and maintain availability of the services provided by the CSD.

10. A CSD shall put in place appropriate procedures concerning human resources to employ, train and retain qualified personnel, as well as mitigate the effects of personnel turnover or overreliance on key personnel.

Article 75

IT tools

1. A CSD shall ensure that its information technology (IT) systems are well-documented and that they are designed to cover the CSD's operational needs and the operational risks that the CSD faces.

The CSD IT systems shall be:

(a) resilient, including in stressed market conditions;

(b) have sufficient capacity to process additional information as a result of increasing settlement volumes;

(c) achieve the service level objectives of the CSD.

2. A CSD systems shall have sufficient capacity to process all transactions before the end of the day even in circumstances where a major disruption occurs.

A CSD shall have procedures for ensuring sufficient capacity of its IT systems, including in the case of the introduction of new technology.

3. A CSD shall base its IT systems on internationally recognised technical standards and industry best practices.

4. A CSD's IT systems shall ensure that any data at the disposal of the CSD is protected from loss, leakage, unauthorised access, poor administration, inadequate record-keeping, and other processing risks.

5. **A CSD's information security framework shall outline the mechanisms that the CSD have in place to detect and prevent cyber-attacks. The framework shall also outline the CSD's plan in response to cyber-attacks.**

6. The CSD shall subject its IT systems to stringent testing by simulating stressed conditions before those systems are used for the first time, after making significant changes to the systems and after a major operational disruption has occurred. A CSD shall, as appropriate, involve in the design and conduct of these tests:

(a) users;

(b) critical utilities and critical service providers;

(c) other CSDs;

(d) other market infrastructures;

(e) any other institutions with which interdependencies have been identified in the business continuity policy.

7. The information security framework shall include:

(a) access controls to the system;

(b) adequate safeguards against intrusions and data misuse;

(c) specific devices to preserve data authenticity and integrity, including cryptographic techniques;

(d) reliable networks and procedures for accurate and prompt data transmission without major disruptions; and

(e) audit trails.

8. The CSD shall have arrangements for the selection and substitution of IT third party service providers, CSD's timely access to all necessary information, as well as proper controls and monitoring tools.

9. The CSD shall ensure that the IT systems and the information security framework concerning the CSD's core services are reviewed at least annually and are subject to audit assessments. The results of the assessments shall be reported to the CSD's management body and to the competent authority.

CSD LINKS

(Article 48(3), (5), (6) and (7) of Regulation (EU) No 909/2014)

Article 84

Conditions for the adequate protection of linked CSDs and of their participants

1. A CSD link shall be established and maintained under the following conditions:

(a) the requesting CSD shall meet the requirements of the receiving CSD's participation rules;

(b) the requesting CSD shall conduct an analysis of the receiving third-country CSD's financial soundness, governance arrangements, processing capacity, operational reliability and any reliance on a third party critical service provider;

(c)the requesting CSD shall take all necessary measures to monitor and manage the risks that are identified following the analysis referred to in point (b);

(d)the requesting CSD shall make the legal and operational terms and conditions of the link arrangement available to its participants allowing them to assess and manage the risks involved;

(e)before the establishment of a CSD link with a third-country CSD, the requesting CSD shall perform an assessment of the local legislation applicable to the receiving CSD;

(f)the linked CSDs shall ensure the confidentiality of information in connection to the operation of the link. The ability to ensure confidentiality shall be evidenced by the information provided by the CSDs, including any relevant legal opinions or arrangements;

(g)the linked CSDs shall agree on aligned standards and procedures concerning operational issues and communication in accordance with Article 35 of Regulation (EU) No 909/2014;

(h)before the link becomes operational, the requesting and receiving CSDs shall:

(i) conduct end-to-end tests;

(ii)establish an emergency plan, as part of the business continuity plans of the respective CSDs, identifying the situations where the securities settlement systems of the two CSDs malfunction or break down, and provide for the remedial actions planned if those situations occur;

(i)all link arrangements shall be reviewed at least annually by the receiving CSD and the requesting CSD taking into account all relevant developments, including market and IT developments, as well as any developments in local legislation referred to in point (e);

(j)for CSD links that do not provide for DVP settlement, the annual review referred to in point (i) shall also include an assessment of any developments that may allow supporting DVP settlement.

For the purposes of point (e), in performing the assessment, the CSD shall ensure that the securities maintained in the securities settlement system operated by the receiving CSD benefit from a level of asset protection comparable to the one ensured by the rules applicable to the securities settlement system operated by the requesting CSD. The requesting CSD shall require from the third-country CSD a legal assessment addressing the following issues:

(i)the entitlement of the requesting CSD to the securities, including the law applicable to proprietary aspects, the nature of the rights of the requesting CSD on the securities, the possibility of encumbering the securities;

(ii)the impact of insolvency proceedings opened against the receiving third- country CSD on the requesting CSD regarding the segregation requirements, settlement finality, procedures and time limits to claim the securities in the relevant third country.

2. In addition to the conditions referred to in paragraph 1, a CSD link providing for DVP settlement shall be established and maintained under the following conditions:

(a)the requesting CSD shall assess and mitigate the additional risks resulting from the settlement

of cash;

(b) a CSD that is not authorised to provide banking-type ancillary services in accordance with Article 54 of Regulation (EU) No 909/2014, and which is involved in the execution of cash settlement on behalf of its participants, shall not receive credit and shall use prefunding mechanisms covered by its participants in relation to the DVP settlements to be processed through the link;

(c) a CSD that uses an intermediary for the cash settlement shall ensure that the intermediary performs that settlement efficiently. The CSD shall conduct yearly reviews of the arrangements with that intermediary.

3. In addition to the conditions referred to in paragraphs 1 and 2, an interoperable link shall be established and maintained under the following conditions:

(a) the linked CSDs shall agree on equivalent standards concerning reconciliation, opening hours for the processing of the settlement and of corporate actions and cut-off times;

(b) the linked CSDs shall establish equivalent procedures and mechanisms for transmission of settlement instructions to ensure a proper, secure and straight through processing of settlement instructions;

(c) where an interoperable link supports DVP settlement, the linked CSDs shall reflect at least daily and without undue delay the results of the settlement in their books;

(d) the linked CSDs shall agree on equivalent risk-management models;

(e) the linked CSDs shall agree on equivalent contingency and default rules and procedures referred to in Article 41 of Regulation (EU) No 909/2014.

Article 85

Monitoring and management of additional risks resulting from the use of indirect links or intermediaries to operate CSD links

1. In addition to complying with the requirements under Article 84, where a requesting CSD uses an indirect link or an intermediary to operate a CSD link, it shall ensure that:

(a) the intermediary is one of the following:

(i) a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 that complies with the following requirements:

— it complies with Article 38(5) and (6) of Regulation (EU) No 909/2014 or with segregation and disclosure requirements at least equivalent to those laid down in Article 38(5) and (6) of Regulation (EU) No 909/2014 where the link is established with a third- country CSD,

— it ensures prompt access by the requesting CSD to the securities of the requesting CSD when required,

— it has low credit risk, which shall be established in an internal assessment by the requesting CSD by employing a defined and objective methodology that does not exclusively rely on external opinions;

(ii) a third-country financial institution that complies with the following requirements:

—it is subject to and complies with prudential rules at least equivalent to those laid down in Regulation (EU) No 575/2013,

—it has robust accounting practices, safekeeping procedures, and internal controls,

—it complies with Article 38(5) and (6) of Regulation (EU) No 909/2014 or with segregation and disclosure requirements at least equivalent to those laid down in Article 38(5) and (6) of Regulation (EU) No 909/2014 where the link is established with a third- country CSD,

—it ensures prompt access by the requesting CSD to the securities of the requesting CSD when required,

—it has low credit risk, based upon an internal assessment by the requesting CSD by employing a defined and objective methodology that does not exclusively rely on external opinions;

(b) the intermediary complies with the rules and requirements of the requesting CSD, as evidenced by the information provided by that intermediary, including any relevant legal opinions or arrangements;

(c) the intermediary ensures the confidentiality of information concerning the operation of the CSD link, as evidenced by the information provided by that intermediary, including any relevant legal opinions or arrangements;

(d) the intermediary has the operational capacity and systems for:

(i) handling the services provided to the requesting CSD;

(ii) sending the CSD any information relevant to the services provided in relation to the CSD link in a timely manner;

(iii) complying with the reconciliation measures in accordance with Article 86 and Chapter IX;

(e) the intermediary adheres to and complies with the risk-management policies and procedures of the requesting CSD and it has an appropriate risk-management expertise;

(f) the intermediary has put in place measures that include business continuity policies and associated business continuity and disaster recovery plans, to ensure the continuity of its services, the timely recovery of its operations and the fulfilment of its obligations in events that pose a significant risk of disrupting its operations;

(g) the intermediary holds sufficient financial resources to fulfil its obligations towards the requesting CSD and to cover any losses for which it may be held liable;

(h) an individually segregated account at the receiving CSD is used for the operations of the CSD link;

(i) the condition referred to in point (e) of Article 84(1) is fulfilled;

(j) the requesting CSD is informed of the continuity arrangements between the intermediary and the receiving CSD;

(k) the proceeds from settlement are promptly transferred to the requesting CSD.

For the purposes of the first indent in point (a)(i), the third indent in point (a)(ii) and point (h), the requesting CSD shall ensure that it can have access to the securities held in the individually segregated account at any point in time. Where an individually segregated account at the receiving CSD is however not available for the operations of a CSD link established with a third-country CSD, the requesting CSD shall inform its competent authority about the reasons justifying the unavailability of individually segregated accounts and shall provide it with the details on the risks resulting from the unavailability of individually segregated accounts. The requesting CSD shall in any case ensure an adequate level of protection of its assets held with the third-country CSD.

2. In addition to complying with the requirements under paragraph 1, when a requesting CSD uses an intermediary to operate a CSD link and that intermediary operates the securities accounts of the requesting CSD on its behalf in the books of the receiving CSD, the requesting CSD shall ensure that:

(a) the intermediary does not have any entitlement to the securities held;

(b) the account in the books of the receiving CSD is opened in the name of the requesting CSD and the liabilities and obligations as regards the registration, transfer and custody of securities are only enforceable between both CSDs;

(c) the requesting CSD is able to immediately access the securities held with the receiving CSD, including in the event of a change or insolvency of the intermediary.

3. Requesting CSDs referred to in paragraphs 1 and 2 shall perform a yearly due diligence to ensure that the conditions referred to therein are fulfilled.

Article 86

Reconciliation procedures for linked CSDs

1. The reconciliation procedures referred to in Article 48(6) of Regulation (EU) No 909/2014 shall include the following measures:

(a) the receiving CSD shall transmit to the requesting CSD daily statements with information specifying the following, per securities account and per securities issue:

(i) the aggregated opening balance;

(ii) the individual movements during the day;

(iii) the aggregated closing balance;

(b) the requesting CSD shall conduct a daily comparison of the opening balance and the closing balance communicated to it by the receiving CSD or by the intermediary with the records maintained by the requesting CSD itself.

In the case of an indirect link, the daily statements referred to in point (a) of the first subparagraph shall be transmitted through the intermediary referred to point (a) of Article 85(1).

2. Where a CSD suspends a securities issue for settlement in accordance with Article 65(2), all CSDs that are participants of or have an indirect link with that CSD, including in the case of interoperable links, shall subsequently suspend the securities issue for settlement.

Where intermediaries are involved in the operation of CSD links, those intermediaries shall establish appropriate contractual arrangements with the CSDs concerned in order to ensure compliance with the first subparagraph.

3. In the event of a corporate action that reduces the balances of securities accounts held by an investor CSD with another CSD, settlement instructions in the relevant securities issues shall not be processed by the investor CSD until the corporate action has been fully processed by the other CSD.

In the event of a corporate action that reduces the balances of securities accounts held by an investor CSD with another CSD, the investor CSD shall not update the securities accounts that it maintains to reflect the corporate action until the corporate action has been fully processed by the other CSD.

An issuer CSD shall ensure the timely transmission to all its participants, including investor CSDs, of information on the processing of corporate actions for a specific securities issue. The investor CSDs shall in turn transmit the information to their participants. That transmission shall include all necessary information for investor CSDs to adequately reflect the outcome of those corporate actions in the securities accounts they maintain.

Article 87

DVP settlement through CSD links

Delivery versus payment (DVP) settlement shall be regarded as practical and feasible where:

(a) there is a market demand for DVP settlement evidenced through a request from any of the user committees of one of the linked CSDs;

(b) the linked CSDs may charge a reasonable commercial fee for the provision of DVP settlement, on a cost-plus basis, unless otherwise agreed by the linked CSDs;

(c) there is a safe and efficient access to cash in the currencies used by the receiving CSD for settlement of securities transactions of the requesting CSD and its participants.

III. CSDR ITS - IMPLEMENTING REGULATION 2017/394[5]

[5] COMMISSION IMPLEMENTING REGULATION (EU) 2017/394 of 11 November 2016 laying down implementing technical standards with regard to standard forms, templates and procedures for authorisation, review and evaluation of central securities depositories, for the

RECORD KEEPING

(Article 29(4) of Regulation (EU) No 909/2014)

Article 11

Format of records

1. A CSD shall retain the records referred to in Article 54 of Delegated Regulation (EU) 2017/392, for all transactions, settlement instructions and orders concerning settlement restrictions that it processes, in the format set out in Table 1 in Annex IV to this Regulation.

2. A CSD shall retain the records referred to in Article 55 of Delegated Regulation (EU) 2017/392, for the positions corresponding to all the securities accounts that it maintains in the format set out in Table 2 in Annex IV.

3. A CSD shall retain the records referred to in Article 56(1) of Delegated Regulation (EU) 2017/392 for the ancillary services that it provides in the format set out in Table 3 in Annex IV.

4. CSD shall retain the records referred to in Article 57 of Delegated Regulation (EU) 2017/392 for activities related to its business and internal organisation in the format set out in Table 4 in Annex IV.

5. For the purposes of reporting to authorities, a CSD shall use a legal entity identifier (LEI) to identify in its records:

(a) a CSD;

(b) CSD participants;

(c) settlement banks;

(d) issuers for which the CSD provides the core services referred to in point 1 or 2 of Section A of the Annex to Regulation (EU) No 909/2014.

6. A CSD shall use a legal entity identifier (LEI) or a bank identifier code (BIC), or other available form of identification for legal persons to identify in its records participants' clients, where they are known to the CSD.

7. A CSD may use any available identifier allowing for the unique identification of natural persons at national level, to identify in its records a participant's clients known to the CSD.

8. A CSD shall use in the records retained by it the ISO codes referred to in Annex IV.

9. A CSD may use a proprietary format only if this format can be converted without undue delay into an open format based on international open communication procedures and standards for messaging and reference data, for the purposes of making available its records to authorities in accordance with Article 29(2) of Regulation (EU) No 909/2014.

---

cooperation between authorities of the home Member State and the host Member State, for the consultation of authorities involved in the authorisation to provide banking-type ancillary services, for access involving central securities depositories, and with regard to the format of the records to be maintained by central securities depositories in accordance with Regulation (EU) No 909/2014 of the European Parliament and of the Council (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.065.01.0145.01.ENG&toc=OJ:L:2017:065:TOC

10. Upon request, a CSD shall provide the competent authority with information referred to in Articles 54 and 55 of Delegated Regulation (EU) 2017/392 by means of a direct data feed. A CSD shall be given sufficient time to implement the necessary measures to respond to such a request.